MATHEMATICS Proceedings A 85 (3), September 20, 1982

On the group of units of $GF(q)[x]/(a(x))$

by T.H.M. Smits

Department of Mathematics, Delft University of Technology, Julianalaan 132, 2628 BL Delft, the Netherlands

Communicated by Prof. W.H. van der Poel at the meeting of January 28, 1982

INTRODUCTION

Let $GF(q)$ be a finite field of $q = p^f$ elements and generated by an element χ of degree f over the p-element field $\mathbb{Z}_p$. We consider the quotient of the polynomial ring $GF(q)[x]$ and the principal ideal generated by the polynomial $a(x)$.

In [2] Claasen derived the structure of the group of units, notation $H(a)$, of this ring. In this paper we give a short proof of his result. Let

$$a(x) = \{a_1(x)\}^{n_1} \cdot \{a_2(x)\}^{n_2} \ldots \{a_e(x)\}^{n_e}$$

be a factorization into irreducible polynomials $a_s(x)$ of degree d_s. We have the well-known canonical isomorphism

$$GF(q)[x]/(a) \cong GF(q)[x]/(a_1^{n_1}) \oplus GF(q)[x]/(a_2^{n_2}) \oplus \ldots \oplus GF(q)[x]/(a_e^{n_e}).$$

For the group of units we have the direct product decomposition

$$H(a) \cong H(a_1^{n_1}) \times H(a_2^{n_2}) \times \ldots \times H(a_e^{n_e}).$$

If $n_s = 1$, then $H(a_s)$ is the cyclic group of order $q^{d_s} - 1$ of the finite field $GF(q^{d_s})$. If $n_s > 1$, then the structure of the group $H(a_s^{n_s})$ is more complicated.

STRUCTURE OF THE GROUP OF UNITS

We thus consider the ring

$$S = GF(q)[x]/(g^n) \quad (n > 1),$$

where the irreducible polynomial $g(x)$ is given by

$$g(x) = x^d + \beta_{d-1}x^{d-1} + \beta_{d-2}x^{d-2} + \ldots + \beta_1 x + \beta_0, \quad \beta_i \in GF(q).$$

The finite ring S has q^{dn} elements and is generated over $GF(q)$ by the elements b and z satisfying

$$z = b^d + \beta_{d-1}b^{d-1} + \ldots + \beta_1 b + \beta_0,$$

$$z^n = 0.$$

Let l be the smallest natural number such that $q^l \geq n$, then the element

$$b^{q^l} = u$$

satisfies the relation

$$u^d + \beta_{d-1}u^{d-1} + \ldots + \beta_1 u + \beta_0 = 0.$$

The subring $L = GF(q)(u)$ is a finite field with q^d elements. The subring

$$L(z) = \{\lambda_0 + \lambda_1 z + \lambda_2 z^2 + \ldots + \lambda_{n-1}z^{n-1} \mid z^n = 0,\ \lambda_i \in L\}$$

contains q^{dn} elements, which equals the number of elements of S, hence

$$S = L(z), \quad z^n = 0.$$

Every unit of S may now be written as

$$\varrho(1 + \lambda_1 z + \lambda_2 z^2 + \ldots + \lambda_{n-1}z^{n-1}),\ \varrho \neq 0, \quad \varrho, \lambda_i \in L,$$

hence the group $H(g^n)$ of units of the ring S may be written as the direct product

$$H(g^n) = A(g^n) \times B(g^n),$$

where $B(g^n)$ is the group of units of the finite field L. So $B(g^n)$ is cyclic of order $q^d - 1$.

The group $A(g^n)$ is of order $q^{d(n-1)}$ and given by

$$A(g^n) = \{1 + \lambda_1 z + \lambda_2 z^2 + \ldots + \lambda_{n-1}z^{n-1} \mid \lambda_i \in L\}.$$

In order to decompose this abelian group into cyclic subgroups we proceed as follows.

The $fd = m$ products $\chi^r u^t$ form a basis $v_1, v_2, \ldots, v_m$ of the finite field L over the prime field $\mathbb{Z}_p$:

$$L = \mathbb{Z}_p v_1 + \mathbb{Z}_p v_2 + \ldots + \mathbb{Z}_p v_m, \quad m = df,\ p^m = q^d.$$

We consider a unit of the form

$$1 + \lambda_k z^k + \lambda_{k+1}z^{k+1} + \ldots + \lambda_{n-1}z^{n-1} \quad (\lambda_k \neq 0).$$

We write

$$k = j \cdot p^s (p \nmid j),\ \lambda_k = \gamma^{p^s} \quad (\gamma \in L),$$

where the unique element γ may be written as

$$\gamma = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_m v_m \quad (\alpha_i \in \mathbb{Z}_p).$$

We now have the following fundamental calculation:

$$(1 + \lambda_k z^k + \lambda_{k+1} z^{k+1} + \ldots + \lambda_{n-1} z^{n-1})(1 + v_1 z^j)^{-\alpha_1 \cdot p^s} \ldots (1 + v_m z^j)^{-\alpha_m \cdot p^s} =$$

$$(1 + \gamma^{p^s} z^k + \lambda_{k+1} z^{k+1} + \ldots + \lambda_{n-1} z^{n-1})(1 + v_1^{p^s} z^k)^{-\alpha_1} \ldots (1 + v_m^{p^s} z^k)^{-\alpha_m} =$$

$$1 + (\gamma^{p^s} - \alpha_1 v_1^{p^s} - \alpha_2 v_2^{p^s} - \ldots - \alpha_m v_m^{p^s}) z^k + \lambda'_{k+1} z^{k+1} + \ldots + \lambda'_{n-1} z^{n-1} =$$

$$1 + (\gamma - \alpha_1 v_1 - \alpha_2 v_2 - \ldots - \alpha_m v_m)^{p^s} z^k + \lambda'_{k+1} z^{k+1} + \ldots + \lambda'_{n-1} z^{n-1} =$$

$$1 + \lambda'_{k+1} z^{k+1} + \ldots + \lambda'_{n-1} z^{n-1} \text{ with new coefficients } \lambda'_{k+1}, \ldots, \lambda'_{n-1} \in L.$$

Hence on multiplying with elements of the form[1]

$$(1 + v_i z^j)^{-\alpha_{ij}}, \; p \nmid j, \quad \alpha_{ij} \in \{0, 1, 2, 3, \ldots\},$$

we may cancel $z, z^2, \ldots, z^{n-1}$ until we arrive at 1, which proves that every element of $A(g^n)$ may be written as

$$1 + \lambda_1 z + \lambda_2 z^2 + \ldots + \lambda_{n-1} z^{n-1} = \prod_{i=1}^{m} \prod_{\substack{j=1 \\ p \nmid j}}^{n-1} (1 + v_i z^j)^{\alpha_{ij}}.$$

The cyclic group

$$A^{(i,j)}(g^n) = \langle 1 + v_i z^j \rangle$$

has order p^{θ_j}, where θ_j is the smallest natural number for which $j \cdot p^{\theta_j} \geq n$.

An easy calculation, cf. [2, Lemma 6.2.1], shows

$$\sum_{\substack{j=1 \\ p \nmid j}}^{n-1} \theta_j = n - 1.$$

The direct product group

$$\prod_{i=1}^{m} \prod_{\substack{j=1 \\ p \nmid j}}^{n-1} A^{(i,j)}(g^n)$$

has order

$$\prod_{i=1}^{m} \prod_{\substack{j=1 \\ p \nmid j}}^{n-1} p^{\theta_j} = p^{m(n-1)} = q^{d(n-1)} = |A(g^n)|,$$

hence the direct product is equal to the group $A(g^n)$:

$$A(g^n) = \prod_{i=1}^{m} \prod_{\substack{j=1 \\ p \nmid j}}^{n-1} A^{(i,j)}(g^n).$$

---

[1] In [2] the notation $u^t z^j = \bar{\sigma}^{t,j}$ is used, i.e. $v_i z^j = \chi^r u^t z^j = \chi^r \bar{\sigma}^{t,j}$.

Denoting the cyclic group of order r by $C(r)$ we have the final result of Claasen [2]:

$$H(g^n) \cong C(q^d - 1) \times A(g^n)$$

$$A(g^n) \cong \prod_{\substack{j=1 \\ p \nmid j}}^{n-1} \underbrace{C(p^{\theta_j}) \times C(p^{\theta_j}) \times \ldots \times C(p^{\theta_j})}_{m = df \text{ factors}}.$$

REMARK. This result is a (difficult to derive) special case of Theorems 2 and 3 of [1].

EXAMPLE 1. We take

$$S = \mathbb{Z}_3[x]/(x^5) = \mathbb{Z}_3(z) \text{ with } z^5 = 0,$$

hence

$$H(x^5) = \{\varrho(1 + \lambda_1 z + \lambda_2 z^2 + \lambda_3 z^3 + \lambda_4 z^4 \mid \varrho \neq 0;\ \varrho, \lambda_i \in \mathbb{Z}_3\} =$$

$$= \mathbb{Z}_3^* \times \langle 1 + z \rangle \times \langle 1 + z^2 \rangle \times \langle 1 + z^4 \rangle =$$

$$\cong C(2) \times C(9) \times C(3) \times C(3).$$

EXAMPLE 2. Let

$$S = \mathbb{Z}_2[x]/(x^2 + x + 1)^2 = \mathbb{Z}_2(b, z),$$

where

$$z = b^2 + b + 1,$$

$$z^2 = 0.$$

With $b^2 = u$, we have $u^2 + u + 1 = 0$, hence

$$L = \mathbb{Z}_2(u) = GF(4);\ v_1 = 1,\ v_2 = u,$$

so

$$S = L(z) = \{\lambda_0 + \lambda_1 z \mid z^2 = 0,\ \lambda_i \in L\}.$$

Finally it follows for the group of units:

$$H\{(x^2 + x + 1)^2\} = \{\varrho(1 + \lambda_1 z) \mid \varrho \neq 0;\ \varrho, \lambda_1 \in L\} =$$

$$= L^* \times \langle 1 + z \rangle \times \langle 1 + uz \rangle =$$

$$\cong C(3) \times C(2) \times C(2).$$

REFERENCES

1. Ayoub, Chr. – On the group of units of certain rings. Journ. Number Theory **4**, 383–403 (1972).
2. Claasen, H.L. – The group of units in $GF(q)[x]/(a(x))$. Indag. Math. **39**, 245–255 (1977).